Community

Follow

Like

Blog Post

Login

RSS Feed

Alessandro Banzer

May 27, 2014 | 2 minute read

Approve/Reject Own Requests

16 11 18,595

To ensure seamless GRC processes it is highly recommended to guarantee that a single user is not allowed to initiated and approve his/her own requests. The principle which stipulates how many users must be involved in approving access requests must be defined by each company and can be slightly different from one to another. This may be a 2, 4 or even 6-Eyes-Principle as given from your management.

In this document I would like to share how we can technically guarantee that a user who initiates the request is not allowed to approve, so that at least the 4-eyes-principle is given.

The following example describes a common set up with four steps.

- Step 1: Request Initiation – Requestor
- Step 2: Manager Approval – Manager
- Step 3: Role Owner Approval – Role Owner
- Step 4: Security Stage – Security Personnel (e.g. SAP Competence Center)

Basically I recommend that the Requestor is not allowed to approve his own requests (neither for his own user nor for requests submitted by him) as Manager at the Manager Stage. As Role Owner he should be allowed to approve requests for his user account and also for requests submitted by him. In case you have different requirements this document gives you a basic idea how this can be handled.

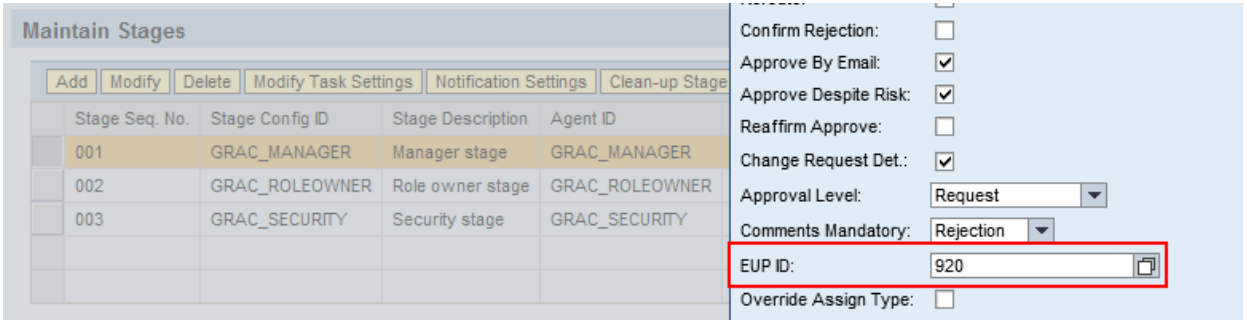
How does the configuration look like?

Go to the IMG Configuration (SPRO) > GRC > Access Control > User Provisioning > Maintain End User Personalization.

I suggest having separate EUP configurations for each stage. Therefore create a new EUP for each stage (Manager, Role Owner and Security). Preferred way is to copy from an existing (e.g. DEFAULT) as most of the settings are available and can be modified easily.

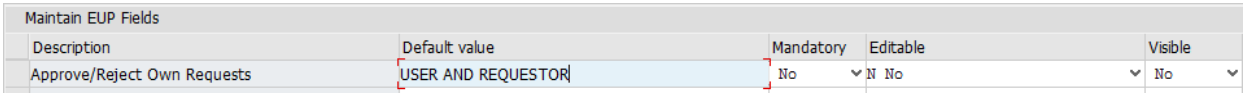
	900	SECURITY_VIEW	Template of Access Request for Security Lead
	910	ROLE_OWNER_VIEW	Template of Access Request for Role Owner
	920	MANAGER_VIEW	Template of Access Request for Manager

The EUP has to be assigned in MSMP configuration for each stage. Below is an example for the Manager Stage with reference to the EUP configuration 920 (Manager View). All others are similar.



The EUP configuration can be defined in different ways:

- If maintained as USER or Blank, the user will not be able to approve his own request
- If maintained as USER AND REQUESTOR, neither user nor requestor can approve the request



Define the field as not editable and not visible as it isn't required to be seen by the approver.

In the Access Request approval screen you will see the error message "You are not allowed to approve your own requests".

As mentioned it is possible to define who can approve/reject own requests at each stage. In my example I have maintained only for Manager Stage as I assume a 4-eyes-principle is sufficient for most of the companies.

Let me know if you need further ideas and do not hesitate to contribute..

Best regards,

Alessandro

Alert Moderator

Assigned Tags

SAP Access Control | approve own requests | Governance Risk And Compliance | governance risk and compliance sap grc | grc 10

Similar Blog Posts

Every option you need to know in MSMP -> Path -> Modify Task Settings

By Rakesh Ram Jun 18, 2016

SAP GRC AC and PC 10.0/10.1/12.0 - Customization of Email Notifications/Variables

By Madhu Babu #MJ Apr 18, 2015

Intelligent Access Control for the Intelligent Enterprise using Machine Learning

By Ravi Mittal Dec 18, 2020

Related Questions

Rejection at Role level in Access Request in GRC 10.1

By Nitesh Kumar Mar 12, 2015

Multiple Role Request Provisioning - GRC AC

By Former Member Sep 30, 2018

how to make comments mandatory in access request 10.1

By shankar p Jan 12, 2020

16 Comments

You must be Logged on to comment or reply to a post.

Former Member
June 29, 2014 at 1:41 pm

Hi,

Thanks a lot for sharing this.. its one of the most basic and critical security requirements while configuring the ARM and i still know several projects where this is still a "Process-Level" understanding rather than a technical setting. Very useful indeed!

Like 0 | Share

Alessandro Banzer | Blog Post Author
June 30, 2014 at 7:13 am

Thanks for your feedback!

Like 0 | Share

Former Member
July 7, 2014 at 4:53 pm

Hi,

Thanks for this blog.

I've a question or concern 🙂 , if the user and the approver both are same then the approval request mail should not be triggered to the approver(i.e. user) how can we configure this ?

Best Regards,

Chaitanya

Like 0 | Share

Alessandro Banzer | Blog Post Author
July 8, 2014 at 7:56 am

Dear Chaitanya,

thanks for your message.

As there is no such check on the submission of an access request there is no standard functionality to avoid that. I am fully aware that restricting the approval is a re-active method, but as there isn't another possibility I suggest to have at least that check to ensure the 4-eyes-principle.

Regards,

Alessandro

Like 0 | Share

Mustafa Motalib

July 18, 2014 at 5:50 am

Hi Alessandro

This is great.

I'm not sure if you can guide me on this.

From our side the "Default value" "Mandatory" & "Editable" fields are greyed out

Description	Default value	Mandatory	Editable	Visible
Approve/Reject Own Requests		Yes	Yes	Yes

Would you know how do i input values there?

Regards

Mustafa

Like 0 | Share

Alessandro Banzer | Blog Post Author

July 18, 2014 at 8:36 am

Dear Mustafa,

thanks for your feedback. For your issue please see note:

http://service.sap.com/sap/support/notes/1673170

Regards,
Alessandro

Like 0 | Share

Former Member
November 3, 2014 at 1:47 pm

Hi Alessandro,

thank you for your post!

This is very helpful.

Can you please let me know if this same setting would work for SPM Log Review workflow.

As i can see that EUPID is not present in Maintain Task settings for SPM Log reiview.

If, not what is the alternative to meet the below requirement.

If the controller is the Firefighter, then system should not allow him/her to approve/reject the Log.

(In other words, FF Controller should not be able to reivew own logs)

Regards,

J

Like 0 | Share

Alessandro Banzer | Blog Post Author
November 3, 2014 at 1:57 pm

Dear J,

thanks for your feedback. As far as I know GRC 10.0 does not allow to assign the same person as controller (parameter 4013/4014).

I have shortly tested in my test-system and while assigning I got the following error message: "Controller and firefighter cannot be the same person"

Does this help?

Regards,

Alessandro

Like 0 | Share

Former Member
November 3, 2014 at 3:36 pm

Hi Alessandro,

Yes, thats correct!

But if The parameters 4013 and 4014 are set to YES, then we can assign controller and firefighter as same.

In this case, when a controller does a FF session and recevies the log for review, he is also able to approve the log. Which should not happen, and unfortunatley, this cannot be controlled by the EUP setting. Do you know if there is a way around for this?

Regards,

J

Like 0 | Share

Former Member
January 25, 2016 at 9:37 am

Hi Alessandro,

Nice document and very well explained.Thanks for all letting us know on this.

I have one question - Do we also have any option where End user can cancel there own request (Which was raised wrongly) from End user link rather only checking status and provisioning log?

Regards,

Abhi

Like 0 | Share

Former Member
September 26, 2016 at 4:20 pm

Great document ! Really, appreciated your work here.

Like 0 | Share

Melanie Hertel
July 3, 2017 at 4:44 pm

Hi Alessandro,

in our case the approver of the first approver stage is the request itself.

So he has to approve request which are created by him.

But in the first approval stage, the user should not be allowed to approve requests for the own user-id.

Therefore, the EUP setting for above for stage one is user and requestor.

The problem is, that this request are staying in his work inbox and must be cancelled by the admin.

Do you know any possibility how the requester can cancel or reject only the request which he has created for the own user-ID?

BR

Melanie

Like 0 | Share

Alessandro Banzer | Blog Post Author
July 15, 2017 at 8:10 am

Hi Melanie,

I guess that's not possible with custom functionality. You might consider a routing rule that reroutes the workflow based on the SOD violation (created by and requested for). You then decide in the routing rule where it will be routed to, e.g. to Security Stage.

Hope that helps.

Cheers, Alessandro

Like 0 | Share

Former Member
August 21, 2017 at 3:23 pm

Dear Alessandro Banzer,

I have a question and need your help..

My requirement is that i want my expert user/Key users to have Access to create Access request for others and also have Access to cancel their own created Access request, if they need to.

Currently it is only the Administrator in GRC who can cancel the Access request,

Can this be achieved through Standard functionalty or we should we go for customisation.

Please suggest, your help is highly appreciated.

Thanks,

Uttam

Like 0 | Share

Alessandro Banzer | Blog Post Author
August 23, 2017 at 5:55 pm

Dear Uttam,

unfortunately, you cannot restrict administrator access to requests created by the user.

Regards, Alessandro

Like 0 | Share

Vaibhav Dubey

April 1, 2021 at 6:42 am

Hii Alessandro,

If we want the role owner to approve their own roles what value should we have for 'Accept/Reject own requests'.

Thanks and regards,

Vaibhav.

Like 0 | Share

Find us on

Privacy	Terms of Use
Legal Disclosure	Copyright
Trademark	Cookie Preferences

Newsletter	Support